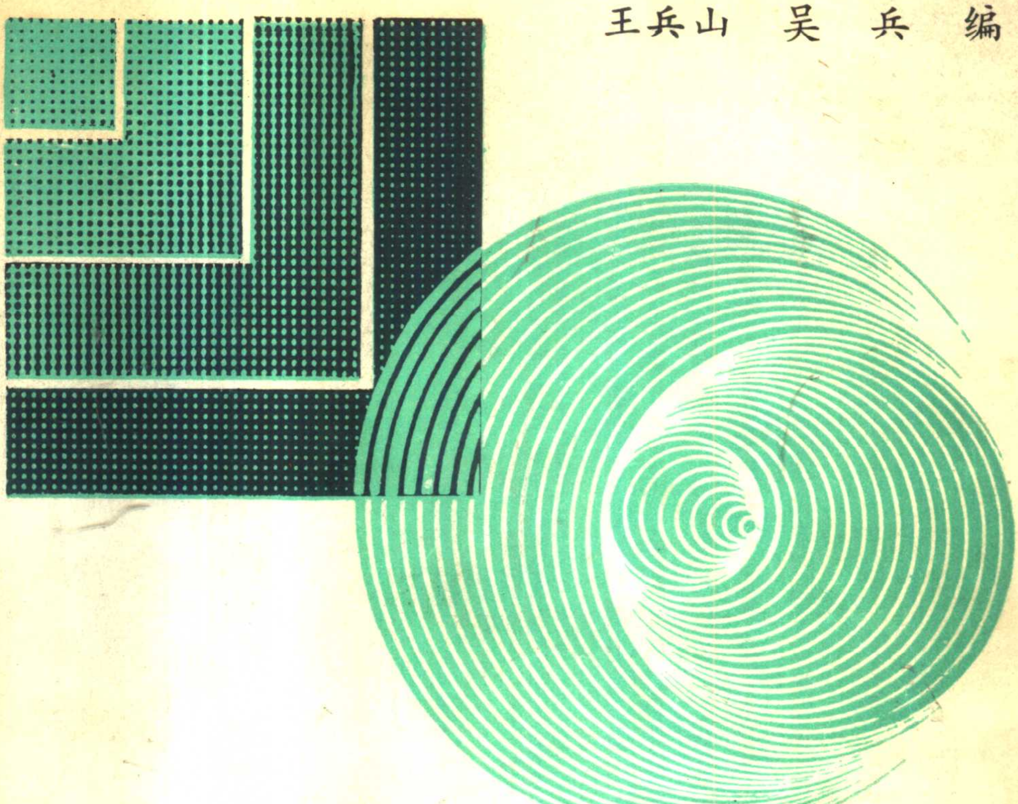
XINGSHI YUYAN

王兵山　吴　兵　编



形式语言

国防科技大学出版社

形式语言

XINGSHI YUYAN

王兵山　吴兵编

国防科技大學出版社　　1988. 6

内 容 提 要

本书是一本关于计算机语言理论的教材，书中系统地介绍了语言理论及自动机理论的基本内容。

全书分八章，主要内容包括：预备知识，文法，正规文法与有穷自动机，上下文无关文法，下推自动机，图灵机，线性界限自动机，确定的上下文无关语言。本书语言简洁，证明严谨，配有大量的例题和习题，便于自学。

本书可作为研究生及高年级本科生教材，亦可供有关专业的研究人员、工程技术人员和大专院校教师参考。

形 式 语 言

王兵山 吴 兵 编

责任编辑 谢小伟

*

国防科技大学出版社 出版发行

湖南省新华书店 经销

国防科技大学印刷厂 印装

*

开本：787×1092 1/16 印张：19 字数：426千

1988年5月第1版 1988年5月第1次印刷 印数：1—5 000 册

ISBN 7-81024-027-7

TP·6 定价：3.15元

前　　言

自动机理论和形式语言理论在计算机科学的发展中曾经起了重要的作用。现在，它们是迅速发展起来的理论计算机的主要分支，对计算机硬件工程和软件工程的发展有重要影响。此外，它们在模式识别等其他科学领域中，也找到了用武之地。

本书只是自动机理论和形式语言理论的一个导引，它是在作者讲授《形式语言与自动机》这门课程的讲义的基础上，加以补充和修改而成的。本课程的重要任务之一，就是培养和训练形式化的思维方式。为了教学的需要，我们尽量照顾理论的系统性，叙述力求严谨，证明力求详尽。为了便于学生理解，书中含有大量例题，这也有助于学生熟悉和掌握本学科中处理问题的方法和技巧。

本书共分八章。第一章介绍本书必须的一些数学概念和工具。第二章介绍文法的形式定义及乔姆斯基谱系，是全书内容的基础。该章给出了较多文法的例子，以便读者尽快掌握和应用。第三、四、五、六、七章按乔姆斯基对文法的分类，逐章介绍正规文法与有穷自动机、上下文无关文法与下推自动机、图灵机与短语结构文法、上下文有关文法及线性界限自动机。这部分是形式语言理论及自动机理论的基本内容。第八章介绍确定的上下文无关语言和确定的下推自动机，该章的内容对计算机编译理论有重要的作用。

各章末均附有足量的习题。其中大部分是基础性的，只要熟悉了教材的基本内容即可做出另一些难度较大、技巧性较强的习题，是用以锻炼读者解题能力的。

由于我们的水平有限，书中谬误及不当之处在所难免，HT望广大读者予以批评指正。

最后，我们衷心地感谢李舟军同志。他认真地审阅了全部书稿，仔细推敲了本书的内容，并以此书为教材进行了教学实践。他发现并纠正了书中不少的错误和不当之处，提出了许多宝贵的意见和建议，为本书付出了大量的辛勤劳动。王金荣同志对本书的编写提出了许多指导意见，作者在此一并致谢。

编　者

1988年2月于长沙

目　录

第一章　预备知识

为了解本书所必须的一些数学基本概念，诸如图、树、网络、集合、关系、函数、自然数（包括Peano公理）、数学归纳法、Monoid、群、同态和同构等等，都能从一般的离散数学书中找到，这里就不再重述了。下面只介绍在一般离散数学书中很少涉及而又为本书所必须的那些数学基本概念，主要包括字母表、字、语言和自由Monoid等。

1.1　字母表、字和语言

无论研究什么问题，总离不开语言，总是通过某种语言进行的。因为通常使用的语言，诸如汉语、英语、俄语、日语，等等，多是在人们长期的社会实践中“自然”地形成的，所以称为“自然语言”。我们知道，这种自然语言种类多，内容丰富，表达能力极强。但是，自然语言也有严重的缺陷，即都不够精确，不够简便，还往往有歧义。为了克服自然语言的这类缺陷，人们就研制了种种人工语言，如数理逻辑中的命题演算和谓词演算，电子计算机的种种程序设计语言（包括电子计算机的指令系统，即所谓的“机器语言”）。这种种人工语言，就是我们所谓的形式语言。

我们的目标是要把形式语言即人工语言定义成一个严格的数学系统，其严格的形式性使得我们能给出形式语言的数学描述，并能进而揭示所描述的语言的结构、特性及其应用范围。

象自然语言一样，形式语言的构成基础也是所谓的“符号”。然而，符号也象几何学中的“点”和“直线”一样，乃是一个没有严格定义的原始概念。因此，我们只能给它以直观描述或说明。当我们把一个记号作为一个整体看待，而不加以分拆时，就称这个记号为一个符号。

常用的符号有以下几种：

i)　数字

　　0　1　2　…　9

ii)　小写拉丁字母

　　a　b　c　…　z

iii)　大写拉丁字母

　　A　B　C　…　Z

iv)　括号

　　‘　’　(　)　[　]　{　}

v)　运算符

　　+　−　×　*　/　÷

vi)　关系符

$$= \quad \neq \quad > \quad \geqslant \quad < \quad \leqslant \quad \in \quad \notin \quad \subset \quad \subseteq$$

vii) 标点符号

$$. \quad , \quad ; \quad :$$

viii) 汉字

下面介绍字母表、字和语言的概念。

定义 1.1.1 我们称符号的非空集合为字母表或符号表，其元素称为字母或符号。▌

有些语言，诸如数理逻辑中的命题演算和谓词演算，其字母表都是无穷集。而种种程序设计语言的符号表，却都是有穷集。它们是常见的较为复杂的字母表的例子。

字母表常用大写的希腊字母Σ表示，而字母表Σ中的元素即符号，则常用较前面的小写拉丁字母 a，b，c，……等表示。

例 1 下列是常用的较简单的字母表：

1) $\{a\}$
2) $\{a, b\}$
3) $\{0, 1\}$
4) $\{a, b, c\}$
5) $\{0, 1, 2\}$
6) $\{0, 1, \cdots, 9\}$
7) $\{a, b, \cdots, z\}$ ▌

例 2 程序设计语言ALGOL_{60}的符号表由以下十一类符号组成：

1) 拉丁字母

   $a \quad b \quad c \quad \cdots \quad z$

   $A \quad B \quad C \quad \cdots \quad Z$

2) 数字

   $0 \quad 1 \quad 2 \quad \cdots \quad 9$

3) 逻辑值

   true **false**

4) 算术运算符

   $+ \quad - \quad \times \quad * \quad / \quad \div \quad \uparrow$

5) 逻辑运算符

   $\neg \quad \vee \quad \wedge \quad \supset \quad \equiv$

6) 关系运算符

   $< \quad \leqslant \quad = \quad \geqslant \quad > \quad \neq$

7) 顺序运算符

   goto **if** **then** **else** **for** **do**

8) 分隔符

   $. \quad , \quad {}_{10} \quad : \quad ; \quad := \quad \sqcup$

   step **until** **while** **comment**

9) 括号

' ' ( ) [ ] { }

begin **end**

10）说明符

boolean **integer** **real** **array** **switch** **procedure** **own**

11）分类符

string **label** **value** ▮

注意，其中黑体字，诸如**true**，**goto**，**for**，**procedure**，**begin**和**string**，等等，称为$ALGOL_{60}$的基本字。每个基本字都是一个不可分割的整体，是一个符号。例如，基本字**begin**和由b，e，g，i和n这五个符号组成的符号串$begin$不同。前者是单个符号，后者为由五个符号组成的符号串。

$ALGOL_{60}$的符号表是一个比较复杂的常用的字母表。

为了方便起见，我们用$\boldsymbol{N}$表示自然数集合，而用$\boldsymbol{I}_+$表示正整数集合。对任意的$n \in \boldsymbol{I}_+$，令

$$\boldsymbol{N}_n = \{0, 1, \cdots n-1\}$$

我们下面接着考虑字母表上的字及字之间的运算及其简单性质，然后再引进语言和语言族的概念。

定义 1.1.2 设Σ为字母表

i) 对任意的$n \in \boldsymbol{N}$及任意的$a_1, \cdots, a_n \in \Sigma$，我们称把$a_1, \cdots, a_n$并置在一起所构成的符号串$a_1 \cdots a_n$为$\Sigma$上的一个字。

ii) 不含任何符号的空符号串（即当$n=0$时的符号串$a_1 \cdots a_n$），称为空字，并用ε表示。

iii) 称集合$\{\alpha \mid \alpha为\Sigma上的一个字\}$为所有$\Sigma$上的字的集合，用$\Sigma^*$表示，并令

$\Sigma^+ = \Sigma^* \backslash \{\varepsilon\}$，$\Sigma_\varepsilon = \Sigma \cup \{\varepsilon\}$。 ▮

通常，我们用小写希腊字母α，β，γ，…或较后面的小写拉丁字母t，u，v，…，z等表示字母表Σ上的字。

例如，当取$\Sigma = \{a, b\}$时，$aabab$和$abbbaba$都是Σ上的字，Σ中的符号a和b也都是Σ上的字。此外，显然还有

$$\Sigma^* = \{\varepsilon, a, b, aa, ab, ba, bb, aaa, \cdots\}$$

和

$$\Sigma^+ = \{a, b, aa, ab, ba, bb, aaa, aab, \cdots\}$$

定义 1.1.3 设Σ为字母表。对任意的α，$\beta \in \Sigma^*$，不妨设：$\alpha = a_1 \cdots a_n$，$\beta = b_1 \cdots b_m (a_1, \cdots, a_n, b_1, \cdots, b_m \in \Sigma)$．若令$\alpha \cdot \beta = a_1 \cdots a_n b_1 \cdots b_m$，就称$\alpha \cdot \beta$为字$\alpha$与字$\beta$的联结，简记为$\alpha\beta$． ▮

定义1.1.3引进的"·"显然是集合Σ^*上的一种二元运算。下面考察这个二元运算的性质。在正式讨论之前，先看下面一个例子。

例 3 取$\Sigma = \{0, 1\}$，$\alpha = 001$及$\beta = 1$，则α，$\beta \in \Sigma^*$，且有

$$\alpha \cdot \beta = 0011 \qquad \beta \cdot \alpha = 1001$$

因此 $\alpha \cdot \beta \neq \beta \cdot \alpha$ ▮

这个例子说明，当$^{\#}\Sigma>1$时，Σ^*上的二元运算“·”并不是可交换的。

定理 1.1.1 设Σ为字母表。如果$S\subseteq\Sigma^*$满足：

i) $\varepsilon\in S$；

ii) 若$\alpha\in S$且$a\in\Sigma$，则$\alpha a\in S$．则有$S=\Sigma^*$．∎

证明 只须证明$\Sigma^*\subseteq S$即可。

若$\alpha\in\Sigma^*$，则有$n_0\in\boldsymbol{N}$及$a_1,\cdots,a_{n_0}\in\Sigma$，使$\alpha=a_1\cdots a_{n_0}$．下面用关于$n$（$0\leqslant n\leqslant n_0$）的归纳法证明如下结论：

若$0\leqslant n\leqslant n_0$，则$a_1\cdots a_n\in S$．

1） 当$n=0$时，由i)可知$a_1\cdots a_n=\varepsilon$，而$\varepsilon\in S$，所以这时命题为真。

2） 对任意的$k\in\boldsymbol{N}_{n_0}$，假定当$n=k$时命题为真，亦即

$$a_1\cdots a_k\in S$$

因为$0\leqslant k<n_0$，所以$0\leqslant k+1\leqslant n_0$．从而再由ii)即知

$$a_1\cdots a_k a_{k+1}=a_1\cdots a_k\cdot a_{k+1}\in S$$

这表明，当$n=k+1$时命题也真。

取$n=n_0$，即有$\alpha=a_1\cdots a_{n_0}\in S$．所以$\Sigma^*\subseteq S$．∎

定理 1.1.2 设Σ为字母表。如果$S\subseteq\Sigma^*$满足：

i) $\varepsilon\in S$；

ii) 若$\alpha\in S$且$a\in\Sigma$，则$a\alpha\in S$．则有$S=\Sigma^*$．∎

这个定理的证明，完全与定理1.1.1类似，留作练习。

定理 1.1.3 设Σ为字母表，$a\in\Sigma$且$\alpha,\beta,\gamma\in\Sigma^*$，则有

i) $\alpha\cdot\beta\in\Sigma^*$，即“·”为$\Sigma^*$上的一个二元运算；

ii) $\alpha\varepsilon=\varepsilon\alpha=\alpha$，即$\varepsilon$为关于该二元运算的么元；

iii) $a\alpha\neq\varepsilon$且$\alpha a\neq\varepsilon$；

iv) $(\alpha\cdot\beta)\cdot\gamma=\alpha\cdot(\beta\cdot\gamma)$；

v) 若$\alpha\beta=\alpha\gamma$，则$\beta=\gamma$；

vi) 若$\alpha\gamma=\beta\gamma$，则$\alpha=\beta$．∎

这个定理不难从定义1.1.2和定义1.1.3，以及定理1.1.1和定理1.1.2直接推出来。

定理 1.1.4 若Σ为字母表，则$\langle\Sigma^*,\cdot,\varepsilon\rangle$为**Monoid**．∎

Monoid意指含么半群。

这可由定理1.1.3的i)、ii)和iv)直接推出来。

根据定理1.1.4，对任意的$\alpha\in\Sigma^*$，若令

$$\alpha^0=\varepsilon$$

$$\alpha^{n+1}=\alpha\cdot\alpha^n \qquad n\in\boldsymbol{N}$$

则有

定理 1.1.5 设Σ为字母表。若$\alpha\in\Sigma^*$，则

i) $\alpha^{n+1}=\alpha^n\cdot\alpha$；

ii) $\alpha^n\cdot\alpha^m=\alpha^{n+m}$；

iii) $(\alpha^n)^m=\alpha^{nm}$．∎

下面，我们再引进几个常用的记号。

定义 1.1.4 设Σ为字母表，$\alpha\in\Sigma^*, L_1\subseteq\Sigma^*$且$L_2\subseteq\Sigma^*$. 则记

$$\alpha\cdot L_1=\{\alpha x \mid x\in L_1\},$$
$$L_1\cdot\alpha=\{x\alpha \mid x\in L_1\},$$
$$L_1\cdot L_2=\{xy \mid x\in L_1 \text{且} y\in L_2\}$$

分别把$\alpha\cdot L_1, L_1\cdot\alpha$和$L_1\cdot L_2$简记为$\alpha L_1, L_1\alpha$和$L_1L_2$. ▌

这时，不难验证有

定理 1.1.6 设Σ为字母表。

i) $\langle 2^{\Sigma^*}, \cdot, \{\varepsilon\}\rangle$ 为 Monoid;

ii) 若$L_1\subseteq\Sigma^*, L_2\subseteq\Sigma^*$，则

$$L_1\cdot L_2=\bigcup_{x\in L_1}xL_2=\bigcup_{y\in L_2}L_1y$$

iii) 若$\alpha, \beta\in\Sigma^*$且$L\subseteq\Sigma^*$,则

$$\alpha(\beta L)=(\alpha\beta)L;$$

iv) 若$\alpha\in\Sigma^*$，$L_1\subseteq\Sigma^*$且$L_2\subseteq\Sigma^*$，则

$$\alpha(L_1\cdot L_2)=(\alpha L_1)\cdot L_2. \quad ▌$$

根据定理1.1.6的i)，若对任意的$L\subseteq\Sigma^*$，令

$$L^0=\{\varepsilon\}$$
$$L^{n+1}=L\cdot L^n \qquad n\in N$$

时，则有

定理 1.1.7 设Σ为字母表，若$L\subseteq\Sigma^*$，则

i) $L^{n+1}=L^n\cdot L$;

ii) $L^n\cdot L^m=L^{n+m}$;

iii) $(L^n)^m=L^{nm}$. ▌

最后，我们再介绍两个概念，即所谓的语言和语言族概念。

定义 1.1.5 设Σ为字母表。

i) 若$L\subseteq\Sigma^*$，则称L为Σ上的一个语言。

ii) 若$\mathscr{L}\subseteq 2^{\Phi^*}$，则称$\mathscr{L}$为$\Sigma$上的一个语言族。

iii) 设L为Σ上的一个语言，若$L=\varnothing$，则称L为空语言；若$^{\#}L<\infty$，则称L为有穷语言；若$^{\#}L=\infty$，则称L为无穷语言。

iv) 设$\mathscr{L}$为Σ上的一个语言族，若$\mathscr{L}=\varnothing$，则称$\mathscr{L}$为空语言族；若$^{\#}\mathscr{L}<\infty$，则称$\mathscr{L}$为有穷语言族；若$^{\#}\mathscr{L}=\infty$，则称$\mathscr{L}$为无穷语言族。▌

设$\Sigma=\{a、b、c、d\}$. 若令

$$L_1=\{a, bd\}$$
$$L_2=\{awb \mid w\in\Sigma^*\}$$
$$L_3=\{a^P \mid P\text{为素数}\}$$
$$L_4=\{a^nb^mc^nd^m \mid n, m\in N\}$$
$$L_5=\{a^nb^nc^n \mid n\in N\}$$

$$L_6=\{w\in\Sigma^*\mid w\text{ 中所含 }a\text{、}b\text{、}c\text{ 的个数之和等于 }w\text{ 中所含 }d\text{ 的个数}\}$$

则$L_1,L_2,\cdots,L_6$都是Σ上的语言，L_1为有穷语言，而$L_2,\cdots,L_6$都是无穷语言。

若再令

$$\mathscr{L}_1=\{L_1,L_2,\cdots,L_6\}$$
$$\mathscr{L}_2=\{\{a^n\cdot w\mid w\in\Sigma^*\}\mid n\in\boldsymbol{N}\}$$
$$\mathscr{L}_3=\{\{w\in\Sigma^*\mid w\text{ 中恰有 }n\text{ 个 }a\}\mid n\in\boldsymbol{N}\}$$

则$\mathscr{L}_1$，$\mathscr{L}_2$和$\mathscr{L}_3$都是Σ上的语言族，$\mathscr{L}_1$为有穷语言族，而$\mathscr{L}_2$和$\mathscr{L}_3$都是无穷语言族。

1.2 自由Monoid

为了进一步揭示字母表的代数性质，我们在此引进自由 Monoid 概念，然后讨论它的性质，并证明一个重要的定理，它允许我们从已知的函数出发，通过原始递归去定义新函数。最后，再利用这个定理引进几个常用的字函数，诸如字的长度和逆字等等。

定义 1.2.1 设 $\langle S,\cdot,e\rangle$ 为 Monoid. 如果存在非空集合 $A\subseteq S$ 满足：

FM_1 $e\notin A$；

FM_2 若$u\in S$且$x\in A$，则$ux\neq e$；

FM_3 若u，$v\in S$和x，$y\in A$，使$ux=vy$，则$u=v$且$x=y$；

FM_4 对任意的$B\subseteq S$，若B满足

i) $e\in B$；

ii) 当$w\in B$，$x\in A$时，有$wx\in B$.

则$B=S$.

这时就称 $\langle S,\cdot,e\rangle$ 为一个自由 Monoid，并称A为它的基。▌

下面我们来看一些例子。

例 1 对自然数集合N上的普通加法运算“+”，显然 $\langle N,+,0\rangle$ 是一个自由 Monoid 共基为集合$\{1\}$. ▌

例 2 对任意的$n\in I_+$，若在N_n上定义模n的加法运算“$+_n$”如下：

$$i+_nj=\begin{cases}i+j & \text{若}i+j<n\\ i+j-n & \text{否则}(i,j\in N_n)\end{cases}$$

则 $\langle N_n,+_n,0\rangle$ 是一个Monoid. 但它不是自由Monoid.

假定它是自由Monoid，它的基为A. 任取 $k\in A$，则有

$$\underbrace{k+_nk+_n\cdots+_nk}_{\text{共 }n\text{ 个 }k}=0$$

这与公理FM_2矛盾。所以 $\langle N_n,+_n,0\rangle$ 决不是自由Monoid. ▌

例 3 对自然数集合N上的普通乘法运算“·”，显然 $\langle N,\cdot,1\rangle$ 是一Monoid.

假定 $\langle N,\cdot,1\rangle$ 是一个自由 Monoid，其基为A，则数 0 和A之间的关系只有以下两种可能：

1) $0\in A$

因为0，$1\in \boldsymbol{N}$ 且 $1\times 0=0=0\times 0$，所以由公理FM_3得$1=0$，这显然不合理。

2) $0\notin A$

取$B=\boldsymbol{N}\setminus\{0\}$，则$1\in B$且$B\subseteq \boldsymbol{N}$．对任意的$w\in B$及$x\in A$，显然有$wx\neq 0$，即$wx\in B$．从而由公理$FM_4$得$B=\mathrm{N}$．这与$0\notin B$矛盾。

总之，由i)和ii)即知，$\langle \boldsymbol{N},\cdot,1\rangle$不是自由Monoid．▮

定理 1.2.1 若Σ为字母表，则$\langle\Sigma^*,\cdot,e\rangle$为一个以$\Sigma$为基的自由Monoid．▮

这可由前一节中定理1.1.2和定理1.1.3直接推出来。

引理 1.1 设A为自由Monoid$\langle S,\cdot,e\rangle$的基。

i) 若$x,y\in A$，则$xy\neq e$；

ii) 若$x,y,z\in A$，则$x\neq yz$；

iii) 若令

$$\bar{A}=\{x_1\cdots x_n \mid n\in \boldsymbol{N}\text{且}x_1,\cdots,x_n\in A\}$$

则$\bar{A}=S$．▮

通常，我们称$\bar{A}$为A的闭包。

证明 首先，i)可由公理FM_2直接推出。

其次，假定有$x,y,z\in A$使$x=yz$．则由公理FM_3及$e\cdot x=yz$得：$e=y,x=z$，因此$e\in A$．这与公理FM_1矛盾。

最后，取$B=\bar{A}$，则$e\in B$且$B\subseteq S$．任取$w\in B$及$x\in A$，由$w\in\bar{A}$知道，必有$n\in \boldsymbol{N}$及$x_1,\cdots,x_n\in A$，使$w=x_1\cdots x_n$．因此$wx=x_1\cdots x_nx\in\bar{A}$，即$wx\in B$．从而由公理$FM_4$得$B=S$，亦即$\bar{A}=S$．▮

引理 1.2 自由Monoid的基是唯一的。

证明 设A_1和A_2为自由Monoid$\langle S,\cdot,e\rangle$的基。

任取$w\in A_1$，因为A_2为基，根据引理1.1的iii)，必有$\bar{A}_2=S$．所以有$n\in \boldsymbol{N}$及$x_1,\cdots,x_n\in A_2$，使$w=x_1\cdots x_n$．但$w\in A_1$且A_1为基，所以$n>0$，亦即$x_n\in A_2$．

对$x_n\in A_2$，通过类似的讨论可知，必有正整数m及$y_1,\cdots,y_m\in A_1$，使$x_n=y_1\cdots y_m$．令$u=x_1\cdots x_{n-1}y_1\cdots y_{m-1}$，则有

$$ew=w=x_1\cdots x_{n-1}y_1\cdots y_m=uy_m$$

从而由公理FM_3得

$$e=u \qquad w=y_m$$

根据公理FM_2，由$x_1\cdots x_{n-1}y_1\cdots y_{m-1}=e$即推出$n=m=1$．因此

$$w=x_1=y_1 \quad \text{即} \quad w\in A_2$$

这表明$A_1\subseteq A_2$．

同理可证得$A_2\subseteq A_1$，所以$A_1=A_2$．▮

引理 1.3 设A为自由Monoid$\langle S,\cdot,e\rangle$的基，$w\in S$且$w\neq e$．

i) 有$u\in S$及$x\in A$，使$w=ux$；

ii) 有$v\in S$及$y\in A$，使$w=yv$．▮

证明 因A为基，根据引理1.1的iii)，则$\bar{A}=S$．所以必有$n\in \boldsymbol{N}$及$x_1,\cdots,x_n\in A$，使$w=x_1\cdots x_n$．但因$w\neq e$，根据公理FM_2，所以还有$n>0$，即$x_n\in A$．这时只要取

$$u = x_1 \cdots x_{n-1} \quad v = x_2 \cdots x_n$$
$$x = x_n \quad y = x_1$$

即有$w = ux$及$w = yv$. ▮

定理1.2.1说明，字母表Σ为自由Monoid $\langle \Sigma^*, \cdot, \varepsilon \rangle$ 的基，而从公理$FM_1 \sim FM_4$和上面三个引理又可看出，自由Monoid 的基也具有字母表的基本性质。因此，我们可以把它看成字母表的推广，这就难怪有人给字母表下了如下的一个定义：

定义 1.2.2 设Σ为自由Monoid$\langle S, \cdot, e \rangle$的基。

i) 称Σ为一个字母表，并称Σ中的元素为符号。

ii) 若$w \in S$，则称w为Σ上的一个字。

iii) 称e为空字，并改记为ε.

iv) 称S为所有Σ上的字的集合，记为Σ^*即$S = \Sigma^*$. ▮

这个定义揭示了字母表的代数本质，使符号、字母表和字有了严格的数学定义。

下面的定理很重要，它告诉我们，在自由Monoid上，可以通过原始递归，从已知函数出发，定义新的函数。

定理 1.2.2 设A为自由 Monoid $\langle S, \cdot, e \rangle$ 的基，M为任意集合，且$m_0 \in M$. 对每个函数$g: M \times S \times A \to M$，皆有唯一的函数$f: S \to M$满足：

i) $f(e) = m_0$;

ii) 若$w \in S$且$x \in A$，则$f(wx) = g(f(w), w, x)$. ▮

证明 1) f的唯一性证明

设函数$f_1: S \to M$和$f_2: S \to M$都满足条件i)和ii). 令

$$B = \{w \in S \mid f_1(w) = f_2(w)\}$$

则$B \subseteq S$.

首先由i)知$f_1(e) = m_0 = f_2(e)$，故而有$e \in B$.

其次，任取$w \in B$及$x \in A$. 由$w \in B$知$f_1(w) = f_2(w)$. 从而由ii)得

$$\begin{aligned} f_1(wx) &= g(f_1(w), w, x) \\ &= g(f_2(w), w, x) \\ &= f_2(wx) \end{aligned}$$

所以$wx \in B$.

综合以上结果，由公理FM_4即得$B = S$. 所以$f_1 = f_2$. 唯一性得证。

2) f的存在性的证明

分六步来完成。

i) 令

$$S_{-1} = \varnothing$$
$$S_0 = \{e\}$$
$$S_{n+1} = S_n \cup \{wx \mid w \in S_n \text{且} x \in A\} \quad (n \in \boldsymbol{N})$$

这时，显然有

$$e \in S_n \text{且} S_n \subseteq S_{n+1} \subseteq S \quad (n \in \boldsymbol{N})$$

因此$\bigcup_{n=0}^{\infty}S_n\subseteq S$. 另一方面，由引理1.1的iii)知道$\bar{A}=S$. 所以对任意的$u\in S$，皆有$n\in \boldsymbol{N}$及$x_1,\cdots,x_n\in A$，使$u=x_1\cdots x_n$. 从而不难由归纳法得到$u\in S_n$. 因此$u\in\bigcup_{n=0}^{\infty}S_n$. 这就表明$S\subseteq\bigcup_{n=0}^{\infty}S_n$.

这样就得到

$$S=\bigcup_{n=0}^{\infty}S_n.$$

ii) 对每个$n\in \boldsymbol{N}$，若函数$\bar{f}: S\to M$满足以下条件：

i′) $\bar{f}(e)=m_0$;

ii′) 对每个$i\in \boldsymbol{N}_n$，若$w\in S_i$且$x\in A$则$\bar{f}(wx)=g(\bar{f}(w), w,x)$. (这里约定$\boldsymbol{N}_0=\varnothing$) 就称$n$为可达的，并称$\bar{f}$达到$n$.

根据这个定义，我们不难由归纳法推出：对任意的正整数n，若$\bar{f}$达到n，且$i\in \boldsymbol{N}_n$，则$\bar{f}\restriction_{S_i}$ ($\bar{f}$在S_i上的限制或称为压缩) 达到i.

iii) 设n，$m\in \boldsymbol{N}$. 若f_1达到n，f_2达到m，且$m\leqslant n$，则f_1为f_2的延拓。

对此，可用关于$m(0\leqslant m\leqslant n)$的归纳法来证明。

首先，当$m=0$时，由条件i′)及$\mathrm{dom}(f_2)=S_0=\{e\}$知道，此时命题为真。

其次，假定对任意的$k<n$，当$m=k$时命题为真，则在$m=k+1$时，由f_2达到m可知，$f_2'=f_2\restriction_{S_k}$达到$k$，根据归纳假设，$f_1$必为$f_2'$的延拓。任取$u\in S_m$，这时，只有以下两种可能：

(a) $u\in S_k$. 因为f_1为f_2'的延拓，所以必有

$$f_1(u)=f_2'(u)=f_2\restriction_{S_k}(u)=f_2(u)$$

(b) 有$w\in S_k$及$x\in A$，使$u=wx$. 因为f_1为f_2'的延拓，所以由条件 ii′)得到

$$\begin{aligned}f_1(u)&=f_1(wx)=g(f_1(w),w,x)\\&=g(f_2'(w),w,x)\\&=g(f_2\restriction_{S_k}(w),w,x)\\&=g(f_2(w),w,x)\\&=f_2(wx)\\&=f_2(u)\end{aligned}$$

总结(a)、(b)即知，f_1确为f_2的延拓。所以当$m=k+1$时，命题也真。

iv) 若$n\in \boldsymbol{N}$为可达的，则仅能有唯一的函数达到n，记为f_n.

实际上，若函数f_1和f_2都达到n，则由iii)知道，f_1为f_2的延拓，同时f_2也为f_1的延拓，所以必有$f_1=f_2$.

v) 每个$n\in \boldsymbol{N}$皆可达。

对此，我们仍用归纳法来证明。

首先，当$n=0$时，因为$S_0=\{e\}$. 当定义函数$f_0: S_0\to M$如下：

$$f_0(e)=m_0$$

时，显然f_0满足条件i′)和ii′)。因此数“0”是可达的。

其次，对任意的 $k\in N$，假定数 k 为可达的，即有函数 $f_k: S_k\to M$ 满足条件i')和ii')．这时，我们可以定义一个函数 $h: S_{k+1}\to M$ 如下：

$$h(u)=\begin{cases} f_k(u) & u\in S_k \\ g(f_k(w),w,x) & u\notin S_k,\text{但有}w\in S_k\text{及}x\in A\text{使}u=wx \end{cases}$$

显然 h 满足条件i')和ii')．所以 h 达到 $k+1$，即数"$k+1$"是可达的。

vi) 因为 $S=\bigcup_{n=0}^{\infty}S_n$，且对每个 $n\in N$ 皆有 $S_n\subseteq S_{n+1}$，所以当令

$$f(u)=f_n(u)\quad u\in S_n\backslash S_{n-1}\quad n\in N$$

时，就得到一个函数 $f: S\to M$，显然这个 f 就满足我们的要求。▮

下面，我们就应用定理1.2.2给出两个重要的函数。

定理 1.2.3 若 A 为自由Monoid $\langle S,\cdot,e\rangle$ 的基，则存在唯一函数 $l: S\to N$ 满足：

i) $l(e)=0$；

ii) 若 $w\in S$ 且 $x\in A$，则

$$l(wx)=l(w)+1.\ ▮$$

证明 若定义函数 $g: N\times S\times A\to N$ 如下：

$$g(n,w,x)=n+1\quad n\in N,w\in S\text{且}x\in A$$

根据定理1.2.2必有函数 $l: S\to N$ 满足i)和ii)．

假定函数 $l': S\to N$ 也满足i)和ii)．令

$$B=\{u\in S\mid l(u)=l'(u)\}$$

显然 $B\subseteq S$．由i)和ii)知 $l(e)=0=l'(e)$，因此 $e\in B$．其次，任取 $w\in B$ 及 $x\in A$，因为 $l(w)=l'(w)$，所以有

$$l(wx)=l(w)+1=l'(w)+1=l'(wx)$$

从而得知 $wx\in B$。但 A 为基，故由公理 FM_4 得 $B=S$，即 $l=l'$．▮

定理 1.2.4 若 A 为自由 Monoid $\langle S,\cdot,e\rangle$ 的基，则存在唯一的函数 $R: S\to S$ 满足：

i) $R(e)=e$；

ii) 若 $w\in S$ 及 $x\in A$，则

$$R(wx)=xR(w).\ ▮$$

证明 若定义函数 $g: S\times S\times A\to S$ 如下：

$$g(u,v,x)=xu\quad u,v\in S\text{且}x\in A$$

则由定理1.2.2知道，必有函数 $R: S\to S$ 满足i)和ii)．

假定函数 $R': S\to S$ 也满足i)和ii)，令

$$B=\{u\in S\mid R(u)=R'(u)\}$$

则 $B\subseteq S$．由i)知 $R(e)=e=R'(e)$，因此 $e\in B$．其次，任取 $w\in B$ 及 $x\in A$，因为有 $R(w)=R'(w)$，故由ii)得

$$R(wx)=xR(w)=xR'(w)=R'(wx)$$

所以 $wx\in B$，但 A 为基，从而由公理 FM_4 得 $B=S$，即 $R=R'$．▮

对任意的自由 Monoid $\langle S,\cdot,e\rangle$，根据引理 1.2，它的基 A 是唯一的，从而由上面

的定理1.2.3和定理1.2.4，我们可以引入以下定义。

定义 1.2.3 设$\langle S, \cdot, e\rangle$为自由Monoid，$w\in S$且$L\subseteq S$.

i) 称$l(w)$为w的长度，记为$|w|$.

ii) 称$R(w)$为w的逆，记为w^R.

iii) 称$\{w^R \mid w\in L\}$为L的逆，记为L^R.其中l和R分别为定理1.2.3和定理1.2.4所给出的函数。▮

现在，我们不难由前面引理1.1和引理1.3以及定理1.2.3和定理1.2.4推出以下结果。

定理 1.2.5 设A为自由Monoid$\langle S, \cdot, e\rangle$的基，则

i) $|e|=0$;

ii) 若$u\in S$，则$|u|\geqslant 0$;

iii) 若$a\in A$，则$|a|=1$;

iv) 若$a_1, \cdots, a_n\in A$，则$|a_1\cdots a_n|=n$;

v) 若$u\in S$且$a\in A$，则$|au|=|u|+1=|ua|$;

vi) 若$u, v\in S$，则$|uv|=|u|+|v|=|vu|$. ▮

定理 1.2.6 设A为自由Monoid$\langle S, \cdot, e\rangle$的基，则

i) $e^R=e$;

ii) 若$a\in A$，则$a^R=a$;

iii) 若$a\in A$且$u\in S$，则$(au)^R=u^Ra$，且$(ua)^R=au^R$;

iv) 若$u, v\in S$，则$(uv)^R=v^Ru^R$;

v) 若$u\in S$，则$(u^R)^R=u$;

vi) 若$a_1, \cdots, a_n\in A$，则$(a_1\cdots a_n)^R=a_n\cdots a_1$. ▮

定理 1.2.7 设$\langle S, \cdot, e\rangle$为自由Monoid，则

i) $\varnothing^R=\varnothing$;

ii) 若$u\in S$且$L\subseteq S$，则$(uL)^R=L^Ru^R$且$(Lu)^R=u^RL^R$;

iii) 若$L_1\subseteq S$且$L_2\subseteq S$，则$(L_1L_2)^R=L_2{}^RL_1{}^R$;

iv) 若$L\subseteq S$，则$(L^R)^R=L$. ▮

以上三个定理的详细证明，留作练习。

下面讨论自由 Monoid 中的“自由”一词的含义到底是指什么。定理1.2.8、定理1.2.9和定理1.2.10回答了这一问题。这三个定理本身在研究自由 Monoid 时是很有用的。

定理 1.2.8 若A为自由Monoid$\langle S, \cdot, e\rangle$的基，$\langle S', *, e'\rangle$为Monoid，则对每个函数$f_0: A\to S'$，都存在唯一的同态$f: S\to S'$，为$f_0$的延拓。▮

定理 1.2.9 设$\langle S, \cdot, e\rangle$为 Monoid，若存在非空集合$A\subseteq S$，使得对任意的Monoid $\langle S', *, e'\rangle$及任意的函数$f_0: A\to S'$，皆有唯一的同态$f: S\to S'$为f_0的延拓。则$\langle S, \cdot, e\rangle$为一个以$A$为基的自由Monoid. ▮

定理 1.2.10 设A为自由Monoid$\langle S, \cdot, e\rangle$的基，$A'$为自由 Monoid $\langle S', *, e'\rangle$的基，若$\# A=\# A'$，则$\langle S, \cdot, e\rangle$和$\langle S', *, e'\rangle$同构。▮